

Appln No. 10/593,026
Amdt date July 8, 2010
Reply to Office action of January 11, 2010

REMARKS/ARGUMENTS

Claims 96-115 are pending. Claims 1-95 are cancelled. Claims 1-3, 100-105, 113, and 114 are amended.

Claims 96-98 and 100-114 are objected to because of informalities. In view of the amendments to the above claims, it is respectfully requested that the above objections be withdrawn.

Claims 96-115 are rejected under 35 U.S.C. § 102 (e) as allegedly being anticipated by U.S. Patent Application Publication No. 2003/0101344 ("Wheeler"). Applicant submits that all of the claims currently pending are patentably distinguishable over the cited references, and reconsideration and allowance of this application are respectfully requested.

The present invention generally concerns secure linking of a record system pointer to a personal authentication device issued to a user via an anonymous public key certificate. The present invention is primarily concerned with assuring anonymity of users with respect to record systems containing information about the users. This way, the links between a user's identity and their personal information are *removed*, while preserving the uniqueness of record system pointers. Thus, the certificate(s) in the present invention anonymously associate a record pointer with the *user*.

In contrast, Wheeler generally concerns the secure linking of: information about a public key enabled device to the public key of that device. (See, for example, paragraph [0017]). That is, in Wheeler, the certificate associates the *device* to a database.

More particularly, amended independent **claim 96** includes, among other limitations, "A method for anonymously indexing an electronic record system," "storing an asymmetric cryptographic private key under the control of a portable storage device of a registered user," "storing an anonymous public key certificate, the anonymous public key certificate being associated with an asymmetric cryptographic public key matching the asymmetric cryptographic private key," and "indexing, within the electronic record system, personal information of the registered user, wherein association of the personal information with the registered user is

Appln No. 10/593,026
Amdt date July 8, 2010
Reply to Office action of January 11, 2010

anonymously verifiable by use of the anonymous public key certificate." Wheeler does not teach the above limitations.

First, Wheeler fails to disclose or suggest a method for "anonymously indexing an electronic record system", as required by claim 96 of the present application. Wheeler's "PuK-Linked Account Database" contains the public keys of the storage devices (see [0108]). Thus, the database of Wheeler will necessarily contain information identifying the devices. Wheeler emphasizes the need for high security of such a database (e.g. [0022], [0029], [0034]). However, the PuK secured account database of Wheeler cannot be considered to be an electronic record system requiring the benefits of the present invention, the nature of such record systems being set out at pages 2 line 13 to page 3 line 6 of the present specification, for example. Rather, the database of Wheeler is a high security store of users' Public keys and a tool to enable the very distinct methodology of Wheeler.

Second, Wheeler does not teach "storing an asymmetric cryptographic private key under the control of a portable storage device of a registered user." The Examiner, in rejecting claim 96, asserts (at page 3, final paragraph) that Wheeler discloses the above limitation at paragraph [0107]. Applicant respectfully disagrees. While Wheeler discloses that "private key 116 (PrK) is retained within the device 104" ([0107]), it is salient to note that this occurs "during its manufacture in the facility 102" and "before the device 104 is released from the secure environment 114", Wheeler [0107]. Prior to release from the secure environment 114, the device of Wheeler is not associated with a person. Wheeler thus fails to disclose "storing an asymmetric cryptographic private key under the control of a portable storage device of a registered user". This reflects the fundamentally different sequence of events required by the Wheeler disclosure as compared with the present invention. In contrast, in the present invention, the private key is associated with the individual, rather than the device, by being stored under the control of the "storage device of a registered user", as recited in claim 96.

Third, Wheeler does not teach "storing an anonymous public key certificate, the anonymous public key certificate being associated with an asymmetric cryptographic public key matching the asymmetric cryptographic private key." The cited "security certificate" described

Appln No. 10/593,026
Amdt date July 8, 2010
Reply to Office action of January 11, 2010

at paragraph [0112] is a public key certificate, NOT an anonymous public key certificate as is required by claim 96 of the present application. Security Certificate SC 126, as seen in Figure 1, is created at Step 608 ([0112], Figure 6) using the device Security Profile 120 [0112]. The purpose of Security Certificate 126 is to enable authentication of the Security Profile of a device [0113]. Wheeler nowhere teaches that Security Certificate 126 is for retaining anonymity, or should be so configured, or might be put to this use. This is in contrast to the anonymous public key certificate utilized in the present invention, which is “associated with an asymmetric cryptographic public key”, and is further configured in a way that enables “association of the personal information with the registered user” to be “anonymously verifiable.” (An example of such anonymous verification being by inclusion of an electronic record pointer in the anonymous public key certificate (claim 99)). Again, Wheeler nowhere teaches or suggests that Security Certificate 126 is anonymous or de-identified, nor that it might be used to anonymously bind a record system pointer to a storage device, and in turn to an individual user associated with that device.

The Office action further asserts that Wheeler, in paragraph [0156], discloses that “the security certificate is linked to a key pair which are both anonymous. The certificate and key pair are linked to a device not a user”. However, it is noted that the “anonymous framework” of Wheeler in [0156] pertains to the distribution of goods and/or services to customers “without regard to any customer-specific information”, “on a per device basis”, “and are not necessarily on a per customer basis”, and “nothing further is required” (see [0142]). That is, Wheeler’s anonymous framework does not relate to storing any personal information of users whatsoever, much less to providing a means for anonymously verifying users’ links to any such information. In particular, Wheeler does not teach in their “anonymous framework” that an anonymous public key certificate containing a record pointer can be used to bind that pointer to a storage device associated with the user, with the effect of in turn allowing personal identifying information to be removed from records pertaining to that user from an electronic records system.

With regard to the assertion that “the security certificate is linked to a key pair which are both anonymous,” it is again important to note that the “security certificate” 120 of Wheeler is

Appln No. 10/593,026
Amdt date July 8, 2010
Reply to Office action of January 11, 2010

not a public key certificate. Not being a public key certificate, there is no suggestion or disclosure that security certificate 120 could contain a copy of a public key and a digital signature thereof. Accordingly a link, if any, from that "security certificate" to any key pair could only be made indirectly, with Wheeler giving no suggestion of how such a link might be effected as this is not the stated purpose of the SC 126.

Fourth, Wheeler does not disclose "indexing, within the electronic record system, personal information of the registered user, wherein association of the personal information with the registered user is anonymously verifiable by use of the anonymous public key certificate." As noted above with respect to paragraphs [0142] and [0156], the "anonymous framework" of Wheeler does not record any personal information of users whatsoever. Also, paragraph [0156] of Wheeler does not teach that "association of the information with the registered user is anonymously verifiable by use of the anonymous public key certificate" because Wheeler's "security certificate" does not pertain to information about the user in a records system.

Moreover, the contents of Wheeler's database are the devices' public keys and a linked Security Profile of the device (e.g. see Wheeler abstract, [0022], [0027], [0032], claims 1 & 10), which destroys anonymity of the device. Inspection of such database contents immediately enables identification of the associated device, by reference to the Security Profile. Wheeler fails to disclose any de-identified (anonymous) database or record system.

Furthermore, the contents of Wheeler's database relate to devices. Many of the devices may not, at a given time, be associated with any individual (the device and key pair being created prior to allocation to any individual), so it is not the case that the database contents are indexed to individuals, rather, the database contents correspond to devices. The database of Wheeler thus does not contain sensitive personal information about *users*, in relation to which anonymity may be desired.

In contrast, in the present invention "association of the personal information with the registered user is anonymously verifiable by use of the anonymous public key certificate." It is therefore not the case that the use of a digital signature alone could make the association verifiable, contrary to such assertion in the Office action.

Accordingly, for at least any of the reasons set out above, claim 96 is not anticipated by Wheeler and therefore is allowable over the cited references.

Independent **claims 103 and 115** includes similar limitations. Consequently, claims 103 and 115 are not anticipated by Wheeler either and therefore are also allowable over the cited references.

Dependent **claims 99 and 106** include the additional limitations of "wherein the indexing comprises associating with each item of personal information of the registered user an electronic record pointer, and wherein the anonymous public key certificate contains the electronic record pointer." It is noted that the Wheeler's paragraph [0165] linking of a public key to a secure database does not involve indexing of personal information of registered users. Therefore, dependent claims 99 and 106 are also allowable over the cited references, as being dependent from an allowable independent claims 96 and 103, respectively and for the additional limitations they include therein.

Dependent **claims 101 and 107** include the additional limitations of "wherein digital signature codes are created for given data items within the electronic record system in order to explicitly link each digitally signed data item to an electronic record pointer associated with the digital signature codes." It is noted that, for at least the reasons set out in the preceding, the use of digital signatures are for entirely different purposes of any digital signatures disclosed by Wheeler. Accordingly, dependent claims 101 and 107 are also allowable over the cited references, as being dependent from an allowable independent claims 96 and 103, respectively and for the additional limitations they include therein.

Dependent **claims 102 and 108** include the additional limitations of "wherein digital signature codes are created for given data items in the electronic record system using the asymmetric cryptographic private key, where each digital signature code is interpreted as explicitly recording the consent of the registered person to the creation of each respective digitally signed data item." It is noted that, for at least the reasons set out in the preceding, the use of digital signatures are for entirely different purposes of any digital signatures disclosed by Wheeler. Thus, dependent claims 102 and 108 are also allowable over the cited references, as

Appln No. 10/593,026
Amdt date July 8, 2010
Reply to Office action of January 11, 2010

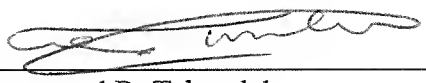
being dependent from an allowable independent claims 96 and 103, respectively and for the additional limitations they include therein.

Dependent **claim 114** include the additional limitations of "wherein the information for associating the registered user with the portable storage device is at least one of: human readable information; and machine readable information." Wheeler nowhere mentions a medical health records database containing user personal information to be updated by health care professionals. The cited paragraph [0132] of Wheeler mentions a "medical provider," which is to merely list a medical provider as one type of service provider who may establish an accounts database. As noted previously herein, Wheeler nowhere discloses de-identified record systems of any description, let alone a medical health records database. Accordingly, dependent claim 114 is also allowable over the cited references, as being dependent from an allowable independent claim 103, and for the additional limitations it includes therein.

Dependent claims 97-102 and 104-114 are dependent from allowable independent claims 96 and 103, respectively and therefore include all the limitations of their base claims and additional limitations therein. Accordingly, these claims are also allowable over the cited references, as being dependent from an allowable independent claim and for the additional limitations they include therein.

In view of the foregoing amendments and remarks, it is respectfully submitted that this application is now in condition for allowance, and accordingly, reconsideration and allowance are respectfully requested.

Respectfully submitted,
CHRISTIE, PARKER & HALE, LLP

By 
Raymond R. Tabandeh
Reg. No. 43,945
626/795-9900

RRT/clv